Listing of Claims:

This listing of claims will replace all prior versions, and listing, of claims in the application.

1. (Currently Amended) A method of authenticating memory devices' data within a gaming machine while said gaming machine is operating, said memory devices' data being authenticated substantially in parallel, said method of authenticating comprising:

reading a next predetermined amount of data from a first memory device storing executable code for operating a wagering game on said gaming machine and graphic data accessed by said executable code to display graphics of said wagering game on a display of said gaming machine;

determining if the next predetermined amount of data is executable code or graphic data;

if said next predetermined amount of data is graphic data, then reading a next predetermined amount of data, without authenticating the graphic data;

if said next predetermined amount of data is executable code, then authenticating said executable code; and

wherein the above steps are repeated substantially continuously while said gaming machine is operating.

2. (Canceled)

3. (Original) The method of claim 1, wherein the method of claim 1 is repeated until said executable code cannot be authenticated.

4. (Original) The method of claim 1, wherein said next predetermined amount of data is a file.

5. (Original) The method of claim 1, wherein said first memory device is a volatile memory device containing a gaming machine program.

6. (Previously Presented) The method of claim 1, wherein if said next predetermined amount of data is said graphic data then determining whether a predetermined amount of events have passed, and wherein if said predetermined amount of events have passed then overriding reading the next predetermined amount of data without authenticating the graphic data and authenticating said graphic data.

7. (Previously Presented) The method of claim 1, further comprising:

reading a next second-predetermined amount of data from a second memory device; and determining whether said next-second predetermined amount of data is authentic;

repeating said reading said next second-predetermined amount of data from the second memory device step and said determining whether said next second-predetermined amount of data step continuously while said gaming machine is operating, wherein said reading said next predetermined amount of data step and said reading said next second-predetermined amount of data step are ~~is~~ performed substantially in parallel.

8. (Previously Presented) The method of claim 1, further comprising

reading a next second-predetermined amount of data from a second memory device;

calculating a hash message digest with said next second-predetermined amount of data; and determining whether all data from said second memory device has been read;

if all data from said second memory device has not been read, then repeating said reading a next second-predetermined step, calculating step and determining whether steps again;

if all data from said second memory device has been read, then using said calculated hash message digest to authenticate the data in said second memory;

wherein said reading said next predetermined amount of data and said reading said next second-predetermined amount of data is performed substantially in parallel.

9. (Previously Presented) The method of claim 1, wherein authentication of said memory devices' data is performed repetitiously within a predetermined amount of time.

10. (Previously Presented) The method of claim 9 wherein said predetermined amount of time is an amount of time that is less than 24 hours.

11-31. (Canceled)

32. (Currently Amended) A method of authenticating data within at least one memory of a gaming machine while the gaming machine is executing a wagering game, said at least one memory storing executable code for operating said wagering game and graphics data accessed by said executable code to display graphics of said wagering game on a display of said gaming machine, said method comprising:

(a) determining if a next predetermined amount of data from said memory is executable code or graphics data;

(b) if said next predetermined amount of data is executable code, then authenticating said executable code and returning to step (a); and

(c) if said next predetermined amount of data is graphics data and a predetermined condition has been met, then authenticating said graphics data and returning to step (a); and if said next predetermined amount of data is graphics data and said predetermined condition has not been met, then returning to step (a) without authenticating said graphics data.

33. (Previously Presented) The method of claim 32, wherein said predetermined condition occurs at predetermined intervals, after a predetermined number of events, or after a predetermined number of times for authenticating said executable code.

34. (Previously Presented) The method of claim 32, wherein said next predetermined amount of data is a file.

35. (Previously Presented) The method of claim 34, wherein data file has an associated verification code.

36. (Previously Presented) The method of claim 35, wherein the associated verification code is a digital signature.

37. (Previously Presented) The method of claim 32, wherein said at least one memory device is a volatile memory device.

38. (Previously Presented) The method of claim 32, further including reading said next predetermined amount of data prior to said determining step.

39. (Previously Presented) The method of claim 38, wherein the authenticating of said executable code includes performing a hash calculation on said read data, said hash calculation providing a result that is used in authenticating said executable code.

40. (Currently Amended) A method of authenticating data within at least one memory of a gaming machine, said at least one memory storing executable code for operating a wagering game on said gaming machine and graphics data accessed by said executable code to display graphics of said wagering game on a display of said gaming machine, said method comprising:

(a) while said gaming machine is booting up, authenticating both the executable code and the graphics data; and

(b) while said gaming machine is executing said ~~a~~ wagering game after booting up:

(i) determining if a next predetermined amount of data from said memory is executable code or graphics data;

(ii) if said next predetermined amount of data is executable code, then authenticating said executable code and returning to step (i); and

(iii) if said next predetermined amount of data is graphics data and a predetermined condition has been met, then authenticating said graphics data and returning to step (i); and if said next predetermined amount of data is graphics data and said predetermined condition has not been met, then returning to step (i) without authenticating said graphics data.

41. (Previously Presented) The method of claim 40, wherein said predetermined condition occurs at predetermined intervals, after a predetermined number of events, or after a predetermined number of times for authenticating said executable code.

42. (Previously Presented) The method of claim 40, wherein said at least one memory device is a volatile memory device.

43. (Previously Presented) The method of claim 40, further including reading said next predetermined amount of data prior to said determining step.

44. (Previously Presented) The method of claim 43, wherein the authenticating of said executable code includes performing a hash calculation on said read data, said hash calculation providing a result that is used in the authenticating of said executable code.

45. (Previously Presented) The method of claim 44, wherein the next predetermined amount of data is a file having an associated verification code.

46. (Previously Presented) The method of claim 45, wherein the associated verification code is a digital signature .

47. (Currently Amended) A method of authenticating data within at least one memory of a gaming machine, said at least one memory storing executable code for operating a wagering game on said gaming machine and graphics data accessed by said executable code to display graphics of said wagering game on a display of said gaming machine, said method comprising:

(a) while said gaming machine is booting up, authenticating both the executable code and the graphics data; and

(b) while said gaming machine is executing said ~~a~~ wagering game after booting up, authenticating said executable code at a first frequency and authenticating said graphics data at a second frequency, said first frequency being greater than said second frequency.

48. (Previously Presented) The method of claim 47, wherein said second frequency is based on a predetermined condition, said predetermined condition occurring at predetermined intervals, after a predetermined number of events, or after a predetermined number of times for authenticating said executable code.

49. (Currently Amended) The method of claim 49 ~~[4]~~, wherein the data file has an associated verification code.

50. (Previously Presented) The method of claim 49, wherein the associated verification code is a digital signature.